REMARKS

Claims 1-10 remain in the case. Reconsideration is respectfully requested based on the comments below.

Claims 5-6 were rejected under 35 U.S.C. 112 for reciting a "type 3 encryption key". According to Claims 5-6, the type 3 encryption key is used in decrypting the read main data. Applicant respectfully submits that the terminology "type 3 encryption key" refers to the unique key SK and is used by the third decrypting unit 204 to decrypt the read main data M_A as claimed (Figures 8 and 10, and Specification page 19 ll. 9-14). The specification paragraph from page 20 line 6 to page 21 line 19 is amended to clarify the unique key SK is considered a type 3 key for encryption and decryption.

Claims 1-4 and 7-10 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Ashe* ("Ashe" U.S. Patent No. 6,014,745) in view of *Marino et al.* ("Marino" U.S. Patent No. 6,026,165). Applicant respectfully traverses this rejection in its entirety.

The present invention as defined in the claims is drawn to a data usage controlling apparatus that limits the usage of encrypted main data according to judgments made on encrypted condition information recorded on the same recording medium as the encrypted main data (Specification page 1 ll. 9-12). The data usage controlling system reads from a recording medium three items: main data that has been encrypted using a type 3 key (Unique key SK), a type 2 key (Supplementary key R_A) that has been encrypted using a type 1 key (Random number R), and condition information that has been encrypted using the type 2 key (Figure 8, and Specification page 13 ll. 6-10, page 19 ll. 9-21 and page 23 ll. 2-7). The type 1 key is read from a predetermined storage unit 201 and is used to decrypt the supplementary key (Specification

page 20 ll. 14-18 and page 23 ll. 7-10). The supplementary key is used to decrypt the usage conditions for the main data which may include an expiry date, a permitted number of executions, or a specified region of use (Specification page 15 ll. 13-17, page 20 ll. 2-3 and 18-21, and page 23 ll. 11-13). If the decrypted usage conditions indicate main data usage is permitted, a unique key (type 3 key) is used to decrypt the digital contents M_A (Figure 10 and Specification page 20 ll. 24-27). Once the main data (digital contents) M_A is used, the data usage controlling system updates the condition information I_A, updates the stored type 1 key, generates a new type 2 key, encrypts the updated condition information using the newly generated type 2 key, encrypts the newly generated type 2 key using the updated type 1 key, and replaces the encrypted type 2 key and the encrypted condition information with an encrypted newly generated type 2 key and an encrypted updated condition information on the recording medium (Figures 10-11, and Specification page 13 ll. 16-24 and page 22 line 20 to page 26 line 1). All of the remaining supplementary keys and condition information for the other digital contents on the recording medium are similarly decrypted, generated/updated, encrypted, and stored (overwritten) on the recording medium to replace the previous values whenever a single digital content is used (Figure 11 and Specification page 21 line 23 to page 22 line 11 and page 25 line 26 to page 26 line 1). Thus, the process of updating the supplementary keys and condition information for each of the digital contents on the recording medium is accomplished for all digital contents every time one of the digital contents is used. In this manner, if the recording medium data were to be restored from a backup, for example, the digital contents would not be usable since the type 1 key is used to decrypt the type 2 key which is used for decrypting the condition information. The type 1 key (Random number R) is updated after the use of any data contents, and hence would not match with the expected type 1 key of the restored recording

medium, and subsequent access is prevented (Fig 14 and Specification page 25 ll. 17-24). In another aspect, if the update to the recording medium were somehow disrupted, the type 1 key is still updated in the executing apparatus and the type 1 key would no longer match the expected type 1 key for subsequent accesses to the recording medium, and subsequent access is prevented (Specification page 26 ll. 4-12). Due to the update of the stored type 1 key in the executing apparatus and the overwriting of the newly encrypted supplementary keys and condition information for each digital content in the recording medium, uncontrolled usage of the digital content is prevented.

Ashe is drawn to a method of accessing proprietary information stored in a remote memory device such as an Electrically Erasable Programmable Read Only Memory (EEPROM) (Ashe col. 1 ll. 36-39). Ashe is addressing the problem of interception of the proprietary data as it is read from the EEPROM, where the proprietary information stored in the remote memory device could be viewed by a hostile third-party if the proprietary information is not protected through encryption. Ashe teaches that a processor reads an encrypted key Zi from a portion of the memory, decrypts Zi into Kc using a master key and a first algorithm (Ashe col. 1 ll. 45-47 and col. 2 line 66 to col. 3 line 1). Once Kc is determined, the proprietary information is decrypted using a second algorithm and may be utilized by the processor in an unlimited manner (Ashe col. 3 ll. 1-6). The master key and first algorithm is shared among all of the processors, so the master key cannot change through an update, for example, or else the system taught by Ashe would fail. Further, Ashe does not disclose any of the operations described above in accordance with the usage of main data governed by condition information such as a permitted number of uses. Ashe teaches a system where once the master key is compromised, unlimited and uncontrolled access is granted to the proprietary information, assuming the decryption algorithms

are known. The Office Action suggests that although Ashe does not disclose and updating means for the condition information and the type 1 key, the generating means for generating a new type 2 key, nor replacing an encrypted key (understood to be only Zi), as an alternative the algorithm unique to the program being encrypted may be encrypted as well. Applicant respectfully submits that the encryption of the second algorithm Ec taught by Ashe is not relevant, and is suggested as an alternative by Ashe in order to safeguard the algorithm and avoid having to store the algorithm in the clear either within the memory. Ashe does not teach changing the algorithm, or updating anything. In fact, Ashe does not teach that the memory itself is writeable by the processor, and it is commonly understood that the "Read Only Memory" EEPROM, prohibits selectively updating of the memory by the processor except perhaps in a non-operational sense where the EEPROM is taken out of ordinary service and reprogrammed.

Marino is drawn to a secure wireless communications system that uses a variable key for encryption and decryption, where the key may be updated based user input along with a sequence number (Marino col. 1 ll. 5-12 and col. 3 ll. 30-35). The sequence number is used to synchronously track the message sequence at both the transmitter and the receiver, and the user may update the re-register a new random number at any time (Marino col. 3 ll. 35-42). Marino teaches a "de-registering" of at least one and possibly all transmitters at the same time (Marino col. 3 ll. 45-48 and col. 4 ll. 31-59). To register any of the transmitters with the receiver, a new random number is generated by the transmitter and sent along with a transmitter identification code to the receiver (Marino col. 3 ll. 54-63). The new random number key is used along with a sequence number to encrypt subsequent messages from the newly registered transmitter to the receiver (Marino col. 3 line 63 to col. 4 line 3). This new random number key and initial sequence number may be encrypted prior to sending, but the encryption and decryption is

accomplished using algorithms and keys that are common to (assumed held within) all receivers and transmitters (Marino col. 4 ll. 3-5). Hence, Marino teaches encryption of messages using a variable key, but that random number key is updated by a user action and is not related to permitted usage of the data itself. Even if it is assumed that the sequence number is analogous to "condition information", the sequence number is used as part of the encryption key and not as encrypted information that governs access to other encrypted information (Marino col. 3 ll. 32-35). Marino does not teach the use or encryption of condition information in accordance with the usage of the read main data, as claimed, which is hypothetically assumed for the sake of analysis to be the transmitted data. As a result, Marino cannot teach an updating means for the condition information. Even if it is assumed for the sake of argument that Marino teaches a type 1 key that is updated, Marino does not teach a generating means for generating a new type 2 key as claimed since the only other encryption taught by Marino is a static encryption of the initial registration message itself using a common key that is not updated. Hence, Marino does not teach either the objects or the effects of the present invention.

Regarding Claim 1, Applicant respectfully submits that even if the cited references are combined as suggested, they do not teach all of the elements of independent Claim 1, as described above. Further, Ashe teaches a system with encryption keys that cannot be updated since the memory itself does not allow a rewriting of data to the location storing the encrypted key Zi. Applicant respectfully submits, therefore, that there is no teaching in the Ashe reference towards an updating of the encrypted key, and to do so would actually defeat the purpose of interchangeability between processors if the key were changed. Applicant submits that it is common within the environment taught by Ashe to exchange a particular EEPROM with another containing different proprietary data. If the encrypted key Zi were updated at any point, the data

would become unusable in subsequent exchanges of the memory device containing the proprietary data.

Independent Claim 9 is a data usage controlling method corresponding with the apparatus of Claim 1 and is believed allowable based on the arguments offered above regarding Claim 1. Similarly, independent Claim 10 is a computer-readable recording medium storing a program corresponding with the apparatus of Claim 1 and is believed allowable based on the arguments offered above regarding Claim 1.

Regarding Claim 2, Applicant respectfully submits that the cited references in any combination do not teach the decrypting means for decrypting all (n-1) encrypted type 2 keys, nor the second encrypting means for encrypting all the (n-1) type 2 keys and replacing all of the encrypted type 2 keys, as claimed. The present invention teaches a synchronization of updating for all of the type 2 keys in order to control usage of all of the data and avoid unauthorized access caused by a possible restoring of saved data, or an interference with the updating of keys. This capability, implemented by the claimed elements above, is neither taught nor suggested by the cited references. Ashe teaches a system where all of the proprietary information is accessible once the encrypted key is decrypted using a common master key. In this manner, Ashe does not teach a plurality of keys, nor that the keys are all updated in synchronization. Applicant respectfully disagrees that Ashe teaches usage control based on condition information associated with the proprietary algorithm because the proprietary algorithm discussed in the cited section relates to simple decryption and passing along the decrypted information to the second processing unit (Ashe Col. 1 ll. 55-65). Ashe does not teach here a condition other than simple decryption, which depends only on possession of the appropriate key and operating the

predetermined decryption algorithm, and does not teach updating or replacing encrypted condition information as claimed.

Marino teaches a plurality of data streams from a plurality of transmitters, but does not teach that all the encryption keys, each registered random number and associated sequence number, is somehow synchronized by encryption with a newly updated single key in order to control usage of all of the data. Further, Marino does not teach two types of keys that are used for encryption separately with a type 2 key being recorded in the recording medium and a type 1 key being stored external to the recording medium. Applicant respectfully submits that even if the cited references are combined as suggested, they do not teach all of the claimed elements of independent Claim 2.

Dependent Claims 3-4 and 7-8 are believed allowable based on their dependence from independent Claim 2, that is believed allowable based on the arguments above.

Based on at least the above arguments, Applicant respectfully requests this rejection be withdrawn.

Claims 5-6 were rejected under 35 U.S.C. 103(a) as being unpatentable over Ashe and Marino in view of Inazawa et al. ("Inazawa" U.S. Patent No. 6,587,948). Applicant respectfully traverses this rejection in its entirety.

Inazawa is drawn to a recording method and apparatus in which digital data is recorded onto a disc as run-length limited code by modulating digital data used for modulating marks or spaces on the disc and, at the same time, the recorded digital data is encrypted by using key data which is also recorded onto the same disc by variation of the shape of marks or spaces with timing having no effect on the edges of the marks and spaces (Inazawa col. 1 ll. 8-15). Inazawa

teaches a recording and playback method where encrypted data is recorded onto an optical disc using a technique that superimposes an the decryption key on the optical encoded elements themselves in a dimension orthogonal to the direction of reading the encrypted data itself (Figures 19A-19D). Even though it is well known to use encryption in general to protect data from illegal copying, Inazawa does not teach the novel usage control techniques to provide controlled access to encrypted content. Inazawa describes the types of copying addressed by his solution as relating to illegal copies produced by using a result of decoding a master key, and illegal copies produced by physically copying a pit form (optical pattern) created on a legal optical disc (Inazawa col. 2 ll. 36-50).

Inazawa is not focused on simple encryption, nor encryption only as a protection against copying, but a particular kind of optical encoding that foils physically copying an optical disc and recovering encrypted data. Applicant respectfully submits that there cannot be any teaching in Inazawa towards the use of the particular type of content encryption encoding that encompasses a condition information that is updated and stored on the optical medium since any alteration of the content data of the optical disc, assuming it can be altered at all, would necessarily change the pit form pattern, and encryption information would be lost. Applicant respectfully submits, therefore, that it is not possible to combine the teachings of Inazawa with the other cited references. Finally, dependent Claims 5-6 are believed allowable based on their dependence from independent Claim 2, that is believed allowable based on the arguments above.

Applicant respectfully requests this rejection be withdrawn.

It is believed that all claims are in condition for allowance, and an early notification of the same is requested.

If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this document and appropriate fee are being deposited with the U.S. Postal Service as first class mail under 37 C.F.R. § 1.8 and is addressed to:
Mail Stop Non-Fee Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

On: April 15, 2004
Date

By: James Lee
Printed Name

Signature

Respectfully submitted,

SNELL & WILMER L.L.P.

Joseph W. Price
Registration No. 25,124
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4920